

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733
Amdt. dated February 15, 2007
Reply to Office Action of August 17, 2006**

New Amendments to the Specification:

Replace the paragraph beginning at col. 6, line 24 with the following:

The results of each sub-task, M_1 , M_2 , and M_3 can be combined to produce the plaintext, M , by a number of techniques. However, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme. Generally, the plaintext M is obtained from the combination of the individual sub-tasks by the following relationship:

$$Y_i \equiv Y_{i-1} + ((M_1 - Y_{i-1})(w_i^{-1} \pmod{p_i}) \pmod{p_i}) \cdot w_i \pmod{n}$$

$$[Y_i = Y_{i-1} + [(M_1 - Y_{i-1})(w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}]$$

where $[i \geq 2] 2 \leq i \leq k$ where k is the number of prime factors of n , and

$$M = Y_k, Y_1 = C_1 \text{ and } w_i = \prod_{j < i} p_j$$

Encryption is performed in much the same manner as that used to obtain the plaintext M , provided (as noted above) the factors of n are available. Thus, the relationship

$$[C = M^e \pmod{n}] \quad C \equiv M^e \pmod{n},$$

can be broken down into the three sub-tasks,

$$[C_1 = M_1^{e_1} \pmod{p_1}] \quad C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$[C_2 = M_2^{e_2} \pmod{p_2}] \quad C_2 \equiv M_2^{e_2} \pmod{p_2} \text{ and}$$

$$[C_3 = M_3^{e_3} \pmod{p_3}] \quad C_3 \equiv M_3^{e_3} \pmod{p_3},$$

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733
Amdt. dated February 15, 2007
Reply to Office Action of August 17, 2006**

where

$$[M_1 = M \pmod{p_1}] \quad \underline{M_1 \equiv M \pmod{p_1}},$$

$$[M_2 = M \pmod{p_2}] \quad \underline{M_2 \equiv M \pmod{p_2}},$$

$$[M_3 = M \pmod{p_3}] \quad \underline{M_3 \equiv M \pmod{p_3}},$$

$$[e_1 = e \pmod{p_1 - 1}] \quad \underline{e_1 \equiv e \pmod{(p_1 - 1)}},$$

$$[e_2 = e \pmod{p_2 - 1}] \quad \underline{e_2 \equiv e \pmod{(p_2 - 1)}}, \text{ and}$$

$$[e_3 = e \pmod{p_3 - 1}] \quad \underline{e_3 \equiv e \pmod{(p_3 - 1)}}.$$